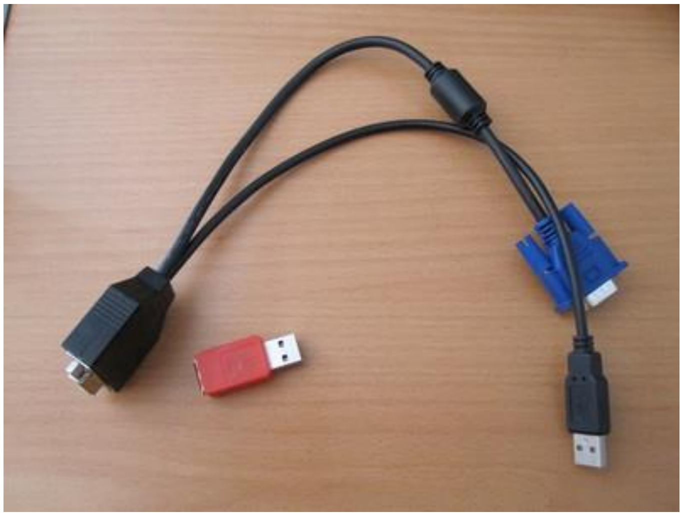
VIDEO GHOST

A while ago I was given this piece of hardware to analyze. It's a scary little bug that sits on the cable between a computer and a monitor and makes screenshots. It comes in HDMI, DVI and VGA (the one I have) flavors and looks more or less like a short extension cable. All of the nasty bits are hidden away in one of the connector housings and the only suspicious thing giving it away is an extra USB cable that goes into it. That is used for power supply when the device is in *stealth* mode, and for reading the captured data afterwards (you need insert the red USB key between the computer and the device in order to access it).

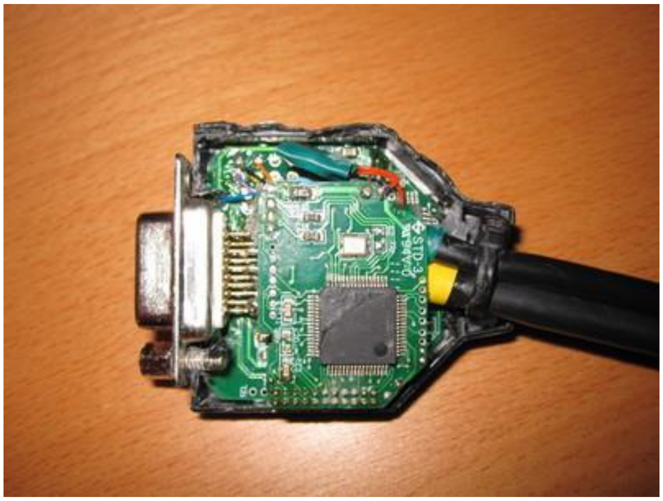
The manufacturer recommends using it on employees and children. In the latter case I hope to teach them how to evade such monitoring should they ever find themselves in a society that encourages that. The use I was exploring though was a bit less sinister capturing of presentation slides on lectures for Viidea.



The first thing I noticed the moment I plugged it in is that my EeePC 901 crashed and required removing the battery to get it to boot again. Trying it again on a different laptop produced similar results. However turning the machine off, plugging the VideoGhost in and turning it on worked.

Since VGA is analog output only that's a bit surprising. I suspected this has something to do with Display Data Channel, which is a fancy name for an I^{2}C bus that's used in all recent monitors for identification. Poking around I quickly found out that all the pins on the middle row of the VGA connector are tied to ground, including pin 9, which is +5 V supply for DDC. Shorting this to the ground while the computer is turned on probably trips some fuses which cause the computer to crash.

I'm not sure whether this is a design or manufacturing error. I also wonder why they haven't used this pin for power supply instead of that suspicious USB cable.



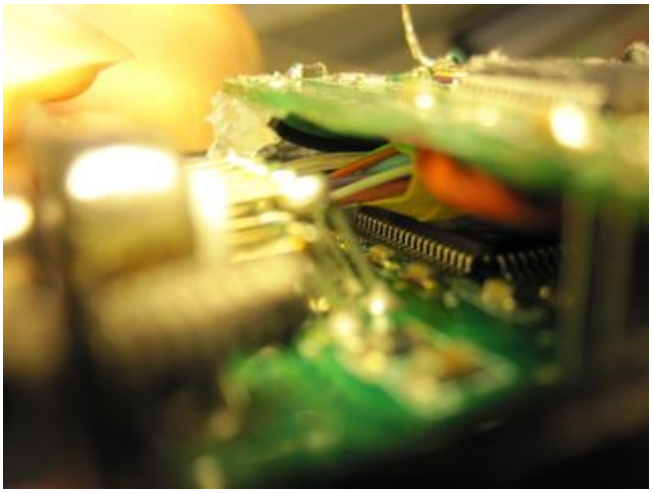
Cracking open the shell wasn't trivial, since the whole thing is filled with hot glue. However a careful application of a hair drier and various sizes of flat screwdrivers did the trick. It still works (minus one SMD capacitor I managed to tear off), however I pretty much demolished the case.

The keelog.com site says the device contains a microprocessor and a FPGA chip. What I see inside more or less agrees with that.

There are two PCBs. The top one contains a chip in a QFP64 package that connects to the USB cable, a MicroSD card (hand soldered via tiny wires) and a backup battery wrapped in green masking tape. All markings are sanded off but it's most likely a microcontroller with hardware USB support. Quite a few ICs fit the description and after some searching around I wasn't able to find one that would fit the pin assignments exactly. I'm sure with some more effort the exact chip could be found. There's also an empty header for what might be a JTAG port.

The bottom board has a chip in a QFP80 package that is connected to the VGA signals. It talks to the top board through something that looks like a combination of a parallel bus and I^{2}C.

Capturing a frame from the VGA requires three AD converters capable of 150 megasamples per second or thereabout. I'm not aware of any off-the-shelf FPGA chips that would contain such hardware. It's possible this is in fact a mass-produced VGA framebuffer IC. It's also possible the bottom side of the PCB contains another IC, but I'm reluctant to find out since it would mean more destructive tearing and I might break something.



I'm not all that impressed by this design. The amazing mess of wires inside doesn't give me confidence in it's reliability, neither does the already-leaking back-up battery inside. It does however offer some interesting challenges in reverse engineering. I might poke around a little more and perhaps try to sniff the I^{2}C communication on the board or checkout that JTAG port. I also wonder what trickery is used in the USB key that enables the USB communication on the device.

Source : https://www.tablix.org/~avian/blog/archives/2011/09/videoghost/